**AMENDMENTS TO CLAIMS:**

Please amend the claims as follows:

1. (Currently Amended) A method for encrypting data, the method comprising:

providing a first data processing system for a first user and a second data processing system for a second user;

providing a session key randomly generated by the second system for use in encrypting original data;

encrypting the data by the second system using the session key and a symmetric encryption routine;

encrypting the session key by the second system, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob;

encrypting the session key by the second system, with a master public key using the asymmetric encryption routine, for storage as a master key blob, wherein the session key is thereby twice encrypted;

storing by the first system a first user private key on any media;

decrypting the user key blob by the first system using the asymmetric encryption routine providing the first system with access to the session key; ~~and~~

the first system decrypting the data using the symmetric encryption routine ~~and~~; and

the second system securely transmitting the data to the first system.

2. – 6. (Canceled)

7. (Previously Presented) The method, as set forth in claim 1, further comprising storing the first user's private key on a data storage medium coupled to a destination data processing system.

8. (Currently Amended) The method, as set forth in claim 1, further comprising storing ~~the~~ a master private key on a data storage medium coupled to the destination data processing system.

9. (Previously Presented) The method, as set forth in claim 7, further comprising retrieving the first user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

10. (Currently Amended) The method, as set forth in claim 7, further comprising retrieving ~~the~~ a master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

11. (Previously Presented) The method, as set forth in claim 1, further comprising utilizing a plurality of public keys and a plurality of private keys.

12. (Currently Amended) A method for encrypting data comprising:

providing a first data processing system for a first user and a second data processing system for a second user;

providing a session key randomly generated by the second system for use in encrypting original data;

encrypting the data by the second system using the session key and a symmetric encryption routine;

encrypting the session key by the second system, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob;

encrypting the session key by the second system, with a master public key using the asymmetric encryption routine, for storage as a master key blob, wherein the session key is thereby twice encrypted;

storing by the first system a first user private key on any media;

decrypting the user key blob by the first system using the asymmetric encryption routine providing the first system with access to the session key; ~~and~~

the first system decrypting the data using the symmetric encryption routine ~~and~~ the second system securely transmitting the data to the first system ~~and~~;; and

a third party gaining access to the data using a master private key to decrypt the master key blob using the asymmetric encryption routine and gain access to the original data.

13.– 17. (Canceled)

18. (Previously Presented) The method as set forth in claim 12, wherein the first user's private key is stored on a data storage medium coupled to the second data processing system.

19. (Currently Amended) The method as set forth in claim 12, wherein ~~the~~ a master private key is stored on a data storage medium coupled to the second data processing system.

20. (Previously Presented) The method as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the first user's private key from a smart card.

21. (Currently Amended) The method as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve ~~the~~ a master private key from a smart card.

22. (Previously Presented) The method as set forth in claim 12, further comprising:

a plurality of private keys; and

a plurality of public keys.

23.– 29. (Canceled)

30. (Currently Amended) A method for encrypting data comprising:

providing a first data processing system for a first user and a second data processing system for a second user;

the second user sending the first user a data file;

the second system randomly generating a session key for use in encrypting original data in the data file;

using the session key, the second system encrypting the data using a symmetric encryption routine;

encrypting the session key by the second system, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob within the encrypted data;

encrypting the session key by the second system with a master public key using the asymmetric encryption routine, for storage as a master key blob within the encrypted data, wherein the session key is thereby twice encrypted;

the second system transmitting the encrypted data to the first system;

storing by the first system a first user private key on any media;

decrypting the user key blob by the first system using the asymmetric encryption routine providing the first system with access to the randomly generated session key;

the first system decrypting the data using the symmetric encryption routine and the second system securely transmitting the data to the first system; and

a third party gaining access to the data using a master private key to decrypt the master key blob using the asymmetric encryption routine and gain access to the original data.